CLAIMS

1. A method for securely transmitting multicast data, comprising:

encrypting at least one title T with at least title key K_T; and

encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$.

2. The method of Claim 1, wherein the channel-unique key K_{cu} is the result of a combination of a channel key K_c and a session key K_s.

3. The method of Claim 2, wherein the combination is a hash function of a concatenation of the channel key K_c and session key K_s.

4. The method of Claim 2, wherein the session key K_s is encrypted with at least a first encryption scheme B^R_{s1} to render a session key block.

5. The method of Claim 4, comprising providing at least one player with device keys K_d to activate the player.

6. The method of Claim 5, comprising providing the player with the channel key K_c.

7. The method of Claim 6, wherein at least one of the providing acts is undertaken in a point-to-point communication.

8. The method of Claim 6, wherein at least one of the providing acts is undertaken as part of a broadcast.

9. The method of Claim 6, comprising providing the player with the session key block.

10. The method of Claim 9, wherein the player can determine the session key K_s from the session key block using the device keys K_d.

11. The method of Claim 10, comprising periodically refreshing the channel key K_c to enforce subscriptions.

12. The method of Claim 10, comprising selectively updating the session key block.

13. The method of Claim 12, comprising updating the session key block by encrypting an updated session key with at least the encryption scheme B^{R}_{s1}.

14. The method of Claim 11, wherein a new channel key K_c' is encrypted with at least a second encryption scheme B^{R}_{s2}.

15. The method of Claim 14, wherein the new channel key K_c' is sent in a message that is split.

16. The method of Claim 14, wherein the new channel key K_c' is refreshed using plural messages.

17. The method of Claim 14, wherein the encryption scheme B^{R}_{s2} includes:

assigning each player in a group of players respective private information I_u;

partitioning players not in a revoked set R into disjoint subsets $S_{i1},...S_{im}$ having associated subset keys $L_{i1},...L_{im}$; and

encrypting the session key K_S with the subset keys $L_{i1},...,L_{im}$ to render m encrypted versions of the session key K_S.

18. The method of Claim 17, wherein the encryption scheme B^R_{s2} further includes partitioning the players into groups $S_1,\ldots,S_w$, wherein "w" is an integer, and the groups establish subtrees in a tree.

19. The method of Claim 18, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

20. The method of Claim 19, wherein the revoked set R defines a spanning tree, and wherein the method includes:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

21. The method of Claim 19, wherein each node has at least one label possibly induced by at least one of its ancestors, and wherein each player is assigned labels from all nodes hanging from a direct path between the player and the root but not from nodes in the direct path.

22. The method of Claim 21, wherein labels are assigned to subsets using a pseudorandom sequence generator, and the act of decrypting includes evaluating the pseudorandom sequence generator.

23. The method of Claim 1, wherein the data is streamed to players.

24. A method for enforcing copy protection compliance and subscription compliance, comprising:

providing players with respective device keys K_d useful for enabling copy protection compliance; and

providing players with at least one channel key K_c useful for enabling subscription compliance, such that a player can decrypt content only if the player is both compliant with copy protection and the player is an active subscriber to a content channel.

25. The method of Claim 24, wherein the content is streamed to players.

26. The method of Claim 25, comprising:

encrypting at least one title T with at least title key K_T; and encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$.

27. The method of Claim 26, wherein the channel-unique key K_{cu} is the result of a combination of the channel key K_c and a session key K_s.

28. The method of Claim 27, wherein the combination is a hash function of a concatenation of the channel key K_c and a session key K_s.

29. The method of Claim 27, wherein the session key K_s is encrypted with at least a first encryption scheme $B^R{}_{s1}$ to render a session key block.

30. The method of Claim 29, comprising providing at least one player with its respective device keys K_d to activate the player.

31. The method of Claim 30, comprising providing the player with the channel key K_c upon or in response to subscription.

32. The method of Claim 30, wherein at least one of the providing acts is undertaken in a point-to-point communication.

33. The method of Claim 30, wherein at least one of the providing acts is undertaken as part of a broadcast.

34. The method of Claim 30, comprising providing the player with the session key block.

35. The method of Claim 34, wherein the player can determine the session key K_s from the session key block using the device keys K_d.

36. The method of Claim 35, comprising periodically refreshing the channel key K_c to enforce subscriptions.

37. The method of Claim 34, comprising selectively updating the session key block.

38. The method of Claim 35, wherein the new channel key K_c' is refreshed by encrypting a new channel key K_c' with at least one encryption scheme.

39. The method of Claim 38, wherein the new channel key K_c' is sent in a message that is split.

40. The method of Claim 38, wherein the new channel key is refreshed using plural messages.

41. A player for decrypting streamed content, comprising:

at least one device key K_d;

means for decrypting a session key K_s using the device key K_d;

means for decrypting a channel unique key K_{cu} using at least the session key K_s; and

means for deriving a title key K_T using at least the channel unique key K_{cu}, the title key K_T being useful for decrypting content.

42. The player of Claim 41, wherein the content is multicast to the player.

43. The player of Claim 42, wherein the player includes means for receiving streamed content, and the content is streamed to the player.

44. A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for receiving private information I_u upon registration with a content provider;

logic means for subscribing to at least one content channel provided by the content provider;

logic means for receiving at least one encrypted channel key K_c at least partially in response to subscribing to the channel;

logic means for deriving the channel key K_c using the information I_u; and

logic means for using at least the channel key K_c to decrypt content streamed over the channel.

45. The computer program device of Claim 44, further comprising:

plural device keys K_d;

logic means for receiving at least one session key block;

logic means for deriving at least one session key K_s from the session key block using at least one device key K_d.

46. The computer program device of Claim 45, further comprising:

logic means for using the session key K_s and channel key K_c to derive a channel unique key K_{cu}; and logic means for using the channel unique key K_{cu} to decrypt a title key K_T useful for decrypting the content.

47. The method of Claim 14, wherein the new channel key K_c' is sent in-band with the title T.

48. The method of Claim 38, wherein the new channel key K_c' is sent in-band with the title T.